Microsoft: Iranian hacking groups join Papercut attack spree

By Sergiu Gatlan

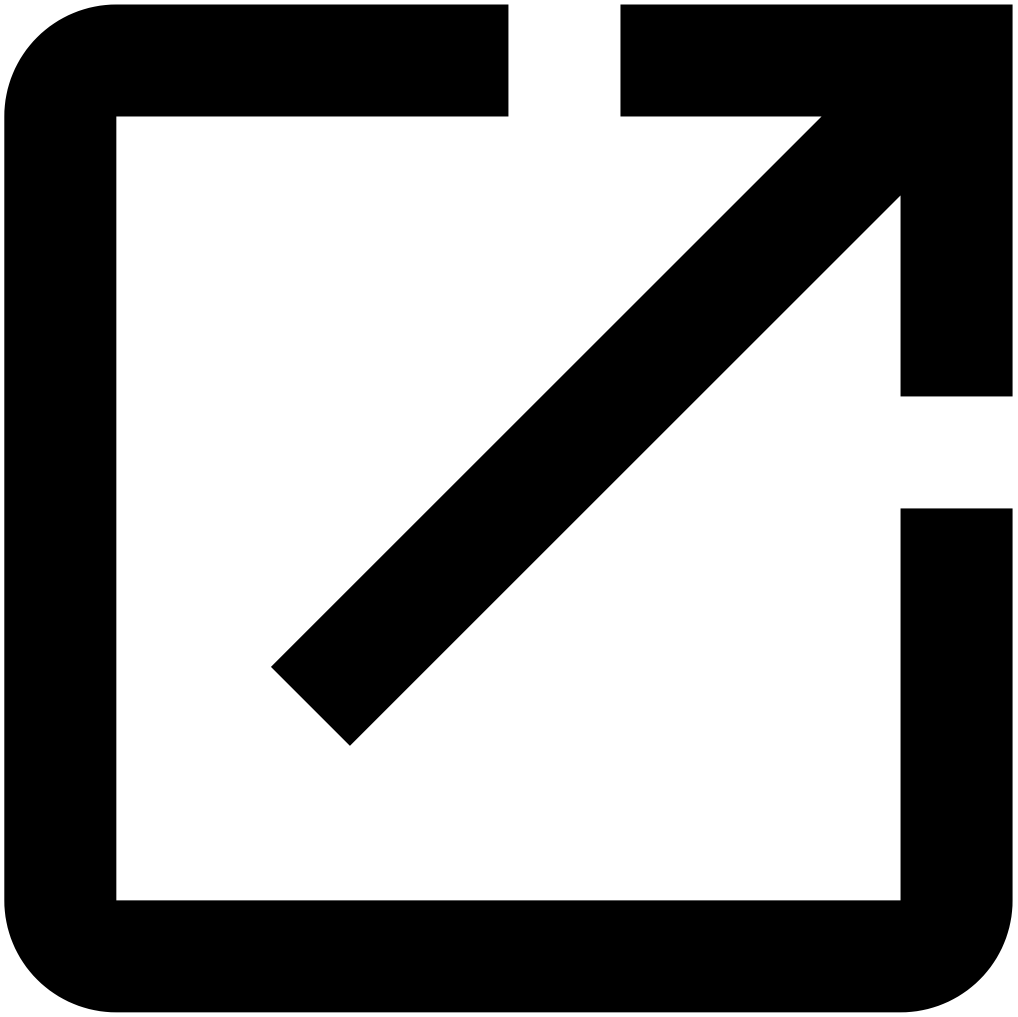
Published: 2023-05-08 · Archived: 2026-04-05 15:03:11 UTC

Microsoft says Iranian state-backed hackers have joined the ongoing assault targeting vulnerable PaperCut MF/NG print management servers.

These groups are tracked as Mango Sandstorm (aka Mercury or Muddywater and linked to Iran's Ministry of Intelligence and Security) and Mint Sandstorm (also known as Phosphorus or APT35 and tied to Iran's Islamic Revolutionary Guard Corps).

"The PaperCut exploitation activity by Mint Sandstorm appears opportunistic, affecting organizations across sectors and geographies," the Microsoft Threat Intelligence team said.


DIE LINKE.
0:00



"Observed CVE-2023-27350 exploitation activity by Mango Sandstorm remains low, with operators using tools from prior intrusions to connect to their C2 infrastructure."

They follow attacks linked to Lace Tempest by Microsoft, a hacking group whose malicious activity overlaps with the FIN11 and TA505 cybercrime gangs connected to the Clop ransomware operation.

Redmond also found that some intrusions led to LockBit ransomware attacks but couldn't provide more information when asked to share additional details.

CISA added this bug to its catalog of actively exploited vulnerabilities on April 21, ordering federal agencies to secure their PaperCut servers within three weeks by May 12, 2023.

The PaperCut vulnerability exploited in these attacks and tracked as CVE-2023-27350 is a pre-authentication critical remote code execution bug in PaperCut MF or NG versions 8.0 or later.

Large companies, state organizations, and education institutes worldwide are using this enterprise printing management software, with PaperCut's developer claiming more than 100 million users from over 70,000 companies.

Security researchers released PoC exploits for the RCE bug soon after the initial disclosure in March 2023, with Microsoft warning several days later that the vulnerability was being used for initial access to corporate networks by the Clop and LockBit ransomware gangs.

While multiple cybersecurity companies have released indicators of compromise and detection rules for PaperCut exploits, VulnCheck shared details on a new attack method last week that can bypass existing detections, allowing attackers to keep exploiting CVE-2023-27350 unobstructed.

"Detections that focus on one particular code execution method, or that focus on a small subset of techniques used by one threat actor are doomed to be useless in the next round of attacks," VulnCheck vulnerability researcher Jacob Baines said.

"Attackers learn from defenders' public detections, so it's the defenders' responsibility to produce robust detections that aren't easily bypassed."

Defenders are encouraged to immediately upgrade theirPaperCut MF and PaperCut NG software to versions 20.1.7, 21.2.11, and 22.0.9 and later, which address this RCE bug and remove the attack vector.

Source: https://www.bleepingcomputer.com/news/security/microsoft-iranian-hacking-groups-join-papercut-attack-spree/